Asian Journal of Applied Science and Technology (AJAST)
Volume 8, Issue 1, Pages 33-46, January-March 2024

Enhancing Electoral Integrity: A Fingerprint-Verified Voting System for Fair and Secure Elections

Gowtham R.[1*], Mohankumar A.[2] & Gokul B.[3]

[1-3]*UG Scholar, IFET College of Engineering, Villupuram, Tamilnadu, India. Email: gowtham996595@gmail.com*[*]

DOI: https://doi.org/10.38177/ajast.2024.8103

Article Received: 21 November 2023 *Article Accepted: 26 January 2024* *Article Published: 12 February 2024*

ABSTRACT

Voting is a significant method through which citizens in democratic nations like India can express their opinions. Voters often use polling booths to cast their ballots. Voting is now done via an electronic voting machine thanks to advancements in technology. This essay discusses a fingerprint-verified voting machine that is Internet of Things based. The primary goals of this project are to decrease voting malpractices and make voting safer with fingerprint verification. Voter information is kept in a database along with their fingerprint. The system verifies the user's Aadhaar number and, if verified, determines whether more than one vote has been cast if the fingerprint matches the stored fingerprint. A "Matching failed" message will appear if the fingerprint matching is incorrect, and an "Aadhar not match" message will appear if the Aadhaar number is incorrect. The controller used in this project is an Arduino Uno. The user's fingerprint is used for authentication. Everybody's fingerprints differ from one another, if not slightly. A notification stating "Already voted" will appear in the event of malpractice. The ballot card is displayed and the result is stored on the cloud using the Arduino IDE for board programming. Only authorized voters may cast ballots, and the system alerts users to instances of fraud. This project ensures fair elections and protects citizens' right to vote.

Keywords: Voting; Fingerprint; Aadhaar; Electronic Voting Machine; Arduino Uno; Fraud Prevention.

1. Introduction

When it comes to a democratic form of government, elections are of the utmost importance, and the integrity of the voting process is of the utmost importance as well. Elections are performed according to predetermined schedules, both in terms of frequency and timing [1]. On top of everything else, the requirement to organize a large number of elections, each of which has its own distinct characteristics and scope, is an additional insult. The democratic system gives individuals the freedom to act and speak freely according to their preferences, as long as they do not violate any laws [2]. As a result of this, individuals are able to freely express their opinions and select their own leaders. The participation of voters is an essential component in ensuring the political system's continued existence over the long term, and electoral voting is an essential component of democracy. Not only should the election process be credible, fair, and objective, but it should also motivate citizens to exercise their right to vote [3]. When a government or organization performs well, it not only facilitates the peaceful transition of power but also strengthens public confidence in it. As society grows more and more reliant on the web and collaboration, citizens are starting to demand higher standards for the way that governments deliver services using contemporary electronic delivery methods [4]. Citizens are aware of the extensive level of adaptability that can be seen in services provided by the private sector, particularly on the Internet. This is the reason why this is the case. The primary considerations of elections and the fundamental nature of a voting system revolve around transparency: it is imperative that regular voters are capable of comprehending and witnessing the process of casting and counting votes, even with minimal education, while also maintaining trust in the system [5].

Should the implementation of electronic voting be carried out, the voting process would become more accessible to millions of additional individuals who are eligible to vote [6]. The increased participation of voters will not only strengthen the credibility of the electoral process, but it will also have the potential to combat the growing prevalence of voter indifference that is observed in a number of democratic nations [7]. It is also acknowledged that more conventional voting techniques will persist for some time, so a way to improve their effectiveness and combine them with the more recent electronic techniques is required. Electing leaders electronically through a web-based application is known as online voting [8].

Online voting offers voters the advantage over the traditional "queue method" in that there is no need to wait in line and they can vote whenever it is convenient for them during the designated election voting period. Also, it reduces the likelihood of errors occurring during the tabulation of votes [9]. Every vote is entered into a database, which can be queried to determine which candidate received the highest number of votes for a particular position. This information can be used to rank the candidates. This system is designed to make the University of Ibadan staff election voting process more credible and user- friendly [10]. It has been observed that low voter turnout has been a problem with the previous voting technique, the Queue System.

2. Literature Survey

In elections, votes are cast and counted using electronic voting machines, or EVMs. Voters use these machines to electronically register their choices rather than traditional paper ballots. The primary processing unit that oversees the entire voting procedure is called the control unit [11]. After a voter's identity is confirmed, it is typically retained by election officials and is in charge of turning on the voting apparatus. In contrast, the voting compartment houses the balloting unit where voters cast their ballots.

By clicking the button next to the party or candidate of their choice on the voting unit, voters engage with the electronic voting machine (EVM). The voter receives a visual cue from the machine confirming that their vote was successfully cast. As opposed to manually tallying paper ballots, electronic voting machines (EVMs) are renowned for their accuracy, speed, and efficiency in the voting process [12]. Nonetheless, disagreements and discussions regarding their dependability have arisen in some areas due to worries about security, tampering, and the absence of a paper trail for verification.

Figure 1. Electronic Voting Machine (EVM)

Elections must be conducted in an honest manner in order for democratic societies to maintain their credibility and stability [13]. Through the implementation of a voting system that utilizes fingerprint verification, it is possible to significantly enhance both the security and validity of elections. By integrating biometric authentication methods, such as fingerprint recognition, into the voting process, this system has the potential to address the persistent issues of voter fraud and identity theft that plague electoral systems all over the world [14]. This would make it extremely difficult, if not impossible, for anyone to cast more than one vote or pretend to be someone else. Voters would be required to scan their unique fingerprints before casting their ballots, which would make it impossible for anyone to do either of those things. It would also make elections more accessible to people with disabilities by providing them with a dependable and user-friendly method of participating in the voting process. This would be accomplished through the implementation of such a system. Individuals would have a higher level of confidence in the voting process if they were able to verify their identity through the use of their fingerprints [15]. This system provides a method that is both open and responsible, which helps to ensure that the results of elections are accurate and that voters' identities are verified and confirmed. The incidence of election fraud and manipulation would be reduced under this system, which would also contribute to the preservation of the fundamental principles of democracy. In addition, this system would strengthen the legitimacy of elected officials. Nevertheless, it is necessary to acknowledge and address concerns regarding breaches of privacy and data security that are associated with the collection and storage of biometric data [16]. For the purpose of ensuring that the voting process is both transparent and accountable, as well as protecting the confidentiality and integrity of voter information, stringent protocols and measures are required. There is the potential for the use of fingerprint verification as a voting method to make elections more trustworthy, to preserve democratic values, and to protect elections in this digital age [17].

Electronic voting machines (EVMs) have faced criticism and concerns regarding several drawbacks. Some of the notable drawbacks include:

Security Concerns: One of the major drawbacks is the potential for security vulnerabilities. EVMs can be susceptible to hacking or tampering, which raises concerns about the integrity of the election process [18].

Lack of Paper Trail: Many electronic voting systems do not produce a verifiable paper trail, making it difficult to audit or recount votes in case of disputes. A paper trail is essential for ensuring the accuracy and integrity of the election results [19].

Complexity and Understanding: Some voters, particularly those unfamiliar with technology or in regions with lower digital literacy, may find it challenging to use electronic voting machines. This can lead to errors or confusion during the voting process [20].

Dependence on Power Supply: Electronic voting machines rely on electricity to function. In areas with unreliable power infrastructure, the potential for disruptions or outages on election day poses a significant concern [21].

Cost: The initial setup cost of electronic voting machines can be high, and the maintenance and software updates also contribute to ongoing expenses. This can be a burden for electoral bodies with limited budgets [22].

Limited Accessibility: People with disabilities may face challenges in using electronic voting machines if they are not designed to be accessible. Ensuring inclusivity in the voting process is crucial [23].

Trust Issues: The lack of transparency in the software and the voting process can lead to a lack of trust among voters [24]. It's important for the electoral authorities to address these concerns to maintain public confidence in the electoral system.

3. Proposed Work

3.1. Finger Based Electronic Voting Machine

Fingerprint-based electronic voting machines (EVMs) are a type of electronic voting machine (EVM) that perform voter authentication and authorization through the utilization of biometric technology, specifically fingerprint scanning. By associating the vote of each voter with their individual fingerprint, the Electronic Voting Machine (EVM) is designed to improve the accuracy and safety of the voting process.

3.1.1. Fingerprint Sensor Module

The R307 fingerprint sensor module is an example of a biometric sensor that was developed specifically with the intention of authenticating each individual user.

Fingerprint Recognition: The primary function of the R307 is to capture and recognize fingerprints. It uses advanced algorithms to convert unique fingerprint patterns into a digital format for comparison.

High Sensitivity: The sensor has a high sensitivity to capture detailed fingerprint images, allowing for accurate identification.

Storage Capacity: Some versions of the R307 come with built-in memory to store fingerprint templates. This enables the module to store and later match fingerprints without relying on external systems.

Communication Interface: The module usually supports communication with external devices through interfaces like UART (Universal Asynchronous Receiver- Transmitter), making it easy to integrate into various projects.

Embedded System Integration: The R307 is often used in embedded systems and microcontroller-based projects. You can connect it to a microcontroller or a single- board computer to enable fingerprint-based authentication in your applications.

Security: Fingerprint recognition is considered a secure method of authentication because each person's fingerprint is unique. The R307's algorithms help ensure reliable and accurate identification.

Application Areas: Common applications include access control systems, time attendance systems, and any other scenario where secure and convenient biometric authentication is required.

3.1.2. Fingerprint Module Working

The R307 fingerprint sensor module is a biometric device that captures and recognizes fingerprints. Here's a basic overview of how it works:

Image Capture: When you place your finger on the sensor, the module captures a high- resolution image of your fingerprint. It typically uses an optical sensor or a capacitive sensor for this purpose.

Image Processing: After that, the picture that was obtained is processed in a manner that separates out the distinctive characteristics of the fingerprint, such as its ridge patterns, bifurcations, and minute points. These characteristics allow for the creation of a one-of-a-kind fingerprint template.

Template Storage: The generated fingerprint template is then stored in the module's memory. This template serves as a reference for future finger print comparisons.

Fingerprint Matching: When you place your finger on the sensor for the purpose of identification or verification, the module immediately takes a new picture and begins the process of creating a fingerprint template.

Comparison: One can make a comparison between the newly created template and the templates that are stored in the database of the module. In the event that a match is found, an action (such as unlocking a device or granting access) is carried out in response to a fingerprint that has been acknowledged.

3.1.3. Verification and Identification Modes

Verification (1:1): In this mode, the module compares the captured fingerprint with a specific pre-enrolled fingerprint.

Identification (1:N): In this mode, the module searches its entire data base to find a match for the captured fingerprint.

Output: The module provides an output signal indicating whether the fingerprint matches an enrolled one or not.

3.2. Application of Fingerprint Module

Access Control Systems: The R307 is commonly used in access control systems for securing buildings and restricted areas. It ensures that only authorized individuals can gain entry by matching their fingerprints with enrolled data.

Time and Attendance Tracking: In workplaces, the R307 is employed for time and attendance systems. Employees can clock in and out by scanning their fingerprints, providing a secure and efficient method for tracking working hours.

Smart Locks for Homes and Offices: Integrated with smart locks, the R307 enables secure access to homes or offices. Users can unlock doors by simply placing their registered fingerprint on the sensor.

Mobile Devices (Smartphones and Tablets): The R307 can be integrated into mobile devices for biometric authentication. It enhances the security of smartphones and tablets by allowing users to unlock their devices and authorize transactions using their fingerprints.

Laptop and Computer Security: Used in laptops and computers, the R307 provides a secure login method. It replaces traditional passwords with biometric authentication, reducing the risk of unauthorized access.

Financial Transactions: The R307 enhances security in financial applications. It can be used for secure authentication in online banking, ensuring that only authorized individuals can access and manage their accounts.

Automated Teller Machines (ATMs): Integrated into ATMs, the R307 adds an extra layer of security to financial transactions. Users can authenticate themselves using their fingerprints before conducting transactions.

Healthcare Systems: In healthcare settings, the R307 controls access to sensitive areas and patient records. It helps maintain the confidentiality of medical information by ensuring that only authorized personnel can access.

Identification Cards and Passport Systems: The R307 can be utilized in the development of biometric identification cards and passports, enhancing the security and authenticity of these documents.

Educational Institutions: Implemented in schools and universities for secure attendance tracking. It ensures that only registered students and staff can access certain areas or services.

Industrial Applications: Used in industrial settings for access control to machinery and secure areas. It adds an additional layer of security to prevent unauthorized access to critical equipment.

3.3. Component Description Arduino UNO

The open-source company Arduino is responsible for the design and production of microcontrollers as well as development kits that combine a single board. Through the utilization of these products, it is possible to create digital devices and interactive objects that are capable of sensing and being controlled digitally in addition to being physically controlled. Both the GNU Lesser General Public License (LGPL) in addition with the GNU General Public License (GPL), which are the licensing requirements for the products, make it possible for anyone to manufacture and distribute the products. You can find more information about these licenses here. Preassembled and do-it-yourself kits are the two types of Arduino boards that are available for purchase in the marketplace. The designs of Arduino boards incorporate a wide variety of controllers and microprocessors into their construction. Connecting to other circuits, shields, or expansion boards can be accomplished through the use of the I/O pins that are located on the boards. Both digital and analog connections can be made to these pins. It is possible to load software from your personal computer onto some of the boards because the serial communications interfaces on some of them are compatible with the Universal Serial Bus (USB).

3.3.1. Programming in Arduino Uno R3

The board's microcontroller comes with a boot loader already installed, so you can upload new code without buying a separate hardware programmer. Using a protocol like STK500 can make this data transmission possible. Bypassing the boot loader and making use of the In-Circuit Serial Programming header is an alternate way to load the program onto the microcontroller.

3.3.2. Buzzer

A piezoelectric sound system is comprised of a piezoelectric diaphragm, which is the primary component responsible for the generation of sound waves. Plates made of piezoelectric ceramic and metal come together to form a piezoelectric diaphragm. Electrodes are placed on either side of the diaphragm. Adhesives are used to secure the two plates, one of which is made of piezoelectric ceramic and the other of which is made of metal. When the electrodes of a piezoelectric diaphragm are subjected to a direct current (DC) voltage, the piezoelectric effect is triggered, which results in mechanical distortion. Regarding an asymmetric piezoelectric element, it has been observed that there is an increase in distortion that is radial in nature. The conventional transistor interfacing circuit is what is utilized in order to connect a buzzer. Bear in mind that in order to establish a common reference, you will need to connect the 0V rails of each and every buzzer power supply that you come into control.

3.3.3. LCD Display

A 16x2 LCD display is a kind of liquid crystal display with two lines and the ability to display 16 characters per line. The display can show alphanumeric characters, symbols, and some simple graphical elements. Typically, a character consists of a 5x8 pixel matrix.

When displaying information in a readable format, these displays are frequently used in electronic projects and devices. They are frequently employed in microcontroller- based projects, embedded systems, and other scenarios that call for a straightforward and portable text display. Generally, a microcontroller or other similar device must be connected to a 16x2 LCD display in order to control it. Multiple pins are used in the connection to carry control, data, ground, and power signals. Data and commands are sent by the microcontroller to the LCD to specify which characters or symbols to display and where to display them. These displays are popular for their simplicity and ease of use, making them a go-to choice for hobbyists and professionals alike in various electronic projects.

3.3.4. Keyboard

Polycarbonate Material: The top layer of the keyboard consists of a polycarbonate membrane. This membrane serves as the outer surface where users press the keys.

Conductive Traces or Pads: Beneath the polycarbonate membrane, there are conductive traces or pads arranged in a matrix. Each key corresponds to a unique set of these traces.

Circuit Completion: When a key is pressed, the polycarbonate membrane flexes downward, causing the conductive pad for that key to connect with other conductive traces, completing a circuit.

Signal Transmission: The completion of the circuit generates an electrical signal. This signal is then interpreted by the keyboard’s controller, which identifies the key pressed based on the specific combination of connected traces.

Keystroke Registration: Once the key-press is identified, the keyboard sends the corresponding signal to the connected computer or device, registering the keystroke and performing the intended action.

Durability: Polycarbonate is chosen for its durability and flexibility. It allows the keyboard to withstand repeated key presses over time without significant wear and tear.

These keyboards are often quieter and more resistant to dust and spills compared to mechanical keyboards due to their membrane design. They also tend to be more cost- effective to produce.

3.3.5. Microcontroller

The ATmega328 is a popular microcontroller chip developed by Atmel, which is now a part of Microchip Technology. It's widely used in various electronic projects and is perhaps best known for being the heart of many Arduino boards, including the Arduino Uno. Here are some key features and details about the ATmega328:

Architecture: The ATmega328 employs a modified Harvard architecture, which includes 32 KB of flash memory for the storage of programs, 2 KB of SRAM for the storage of data, and 1 KB of EEPROM for the storage of non-volatile data.

Clock Speed: It operates at a clock speed of 16 MHz, allowing for relatively fast execution of instructions.

Peripherals: The ATmega328 has a range of built-in peripherals, including digital and analog I/O pins, SPI (Serial Peripheral Interface), UART (serial communication), I2C (Inter-Integrated Circuit), timers, and more.

Arduino Compatibility: As mentioned earlier, the ATmega328 is widely used in Arduino boards, making it accessible for hobbyists and developers. The bootloader on the chip allows for easy programming through a USB-to- serial interface.

Low Power Consumption: It has various power-saving modes, making it suitable for battery-powered applications.

Processor Core: An 8-bit AVR processor core is incorporated into the device. This processor core is well-known for its efficient set of instructions and low energy consumption capabilities. It is possible to streamline and speed up the execution of instructions by utilizing the RISC architecture, which stands for Reduced Instruction Set Computing.

Flash Memory: There is a flash memory on the ATmega328 that is specifically designated for the firmware, and it is 32 KB in size. You will be able to locate the directory in which you saved your Arduino programming sketch here. One of the most distinguishing characteristics of flash memory, which is characterized by its non-volatile nature, is its ability to store data even when there is no power available..

The "PU" in "**ATmega328-PU**" refers to the package type. In this case, "PU" stands for "plastic, through-hole, and unmarked." The through-hole package means that it's designed for mounting on a printed circuit board (PCB) with leads passing through holes for soldering.

Developers often use the ATmega328 for a wide range of projects, from simple LED blinking experiments to more complex applications like sensor interfacing, robotics, and automation.

Microcontrollers are frequently found in embedded systems, which are systems integrated into larger devices that carry out specific tasks. They are present in many commonplace appliances, including washing machines, microwaves, smart home appliances, and, of course, the central component of well-known development platforms like Arduino and Raspberry Pi. Because of their small size and versatility, they offer a reliable and affordable solution for a variety of applications.

Printed on a single semiconductor chip, integrated circuits (ICs) are miniature electronic circuits made up of several interconnected parts like transistors, resistors, capacitors, and other electronic elements.

3.4. Methodology Circuit Diagram

An Arduino microcontroller for project management, a 16x2 LCD for voter instructions and results display, a buzzer for alerts, indicator LEDs, and a push button for enrollment, deletion, ID selection, and voting make up the core circuitry of this fingerprint-based voting machine project. When the system is prepared to accept votes or show results, a green LED will appear; when the fingerprint module is ready to take a picture of the user's finger, a yellow LED will be visible.

Every pin on the Arduino, including the ones for ENROL, DEL, UP, DOWN, and Match (A0, A1, A2, and A5, respectively), is directly connected to the push button. This connection connects the push button to every pin on the Arduino. In addition, the push button is directly connected to Can1 (via D5), Can2 (via D4), Can3 (via D3), and Result (via D2), all of which are associated with the push button. In order to connect the yellow LED (digital pin D7) of the Arduino to ground, a resistor with a value of one kilo ohm is an absolute requirement. The ground pin of the Arduino is connected to the green LED (digital pin D6) through the use of a single resistor. Direct connections have been made between the Rx and Tx pins of the fingerprint module and the Tx and Rx serial pins of the Arduino.

In order for the fingerprint module on the Arduino board to function correctly, it requires a voltage of 5 volts. In addition, a buzzer can be found at position A5, which is the fifth position. A 16x2 LCD has its RS, EN, D4, D5, D6, and D7 pins directly connected to the digital pins D13, D12, D11, D10, and D8 of an Arduino that is operating in 4-bit mode. These pins are also connected to the D7 pin of the LCD. On the Arduino, you will find each and every one of these pins.

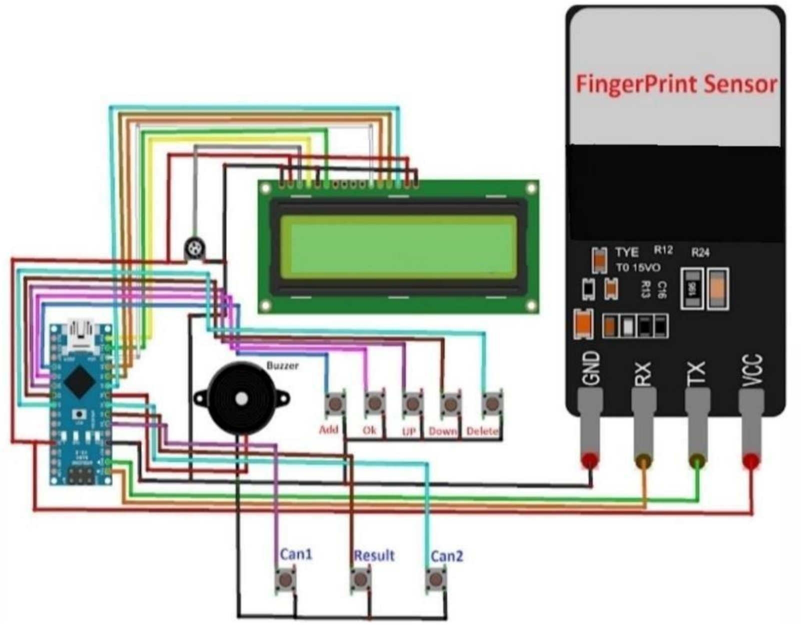

Figure 2. Circuit diagram

3.4.1. Working Explanation

Those who are not familiar with the operation of this biometric voting system for elections may find it difficult to accomplish. The user is required to register their fingerprint or voter information at the beginning of the process. The code permits a maximum of 25 potential voters to participate. This can be accomplished by using either keys or push buttons. Please note that the user is required to press the ENROLL button in order to accomplish this. The subsequent step involves the LCD screen displaying a message that asks the user to input the ID or location where the fingerprint will be saved. This step is followed by the subsequent step. At this point, the user is required to input the ID (Location) by using the up and down arrow keys on their keyboard. Immediately following the selection of a Location/ID, the user is required to press the OK key, which is also referred to as the DEL key. During the course of the procedure, a prompt will appear on the LCD screen, requesting that the user maintain their finger over the fingerprint module. Additionally, the user is required to press their finger onto the fingerprint module in order for it to function properly. Following that, a prompt on the LCD screen will appear, instructing the user to remove their finger from the fingerprint module. In the following step, they will make adjustments to the manner in which their finger is inserted into the module. It is necessary for the user to freely move his finger around on the fingerprint module in order to complete the process. An image is captured by the finger print module, which then converts it into templates. These templates are then saved in the memory of the module under a specific ID that the user selects. Currently, the process of voter registration will be carried out, which will allow individuals to exercise their right to vote. Everyone who is eligible to vote can be registered into the system by following the same procedure.

3.4.2. Voting Process

Right now, the match key is the only way for the user to cast their vote. Immediately following the occurrence of an audible signal, LED illumination, and LCD display of the message, the user will be given the instruction to place their finger on the fingerprint module. For the next three opportunities, you will have the opportunity to place your finger on the Arduino interface. When a user presses their finger against the surface of the fingerprint module, the module takes a picture of the user's finger and then checks the system to determine whether or not the user is a known individual. "Authorized Voter" will be displayed on the liquid crystal display (LCD) if a fingerprint ID is detected. What this indicates is that the user is eligible to cast a vote. Voting is the next step in the process, which comes after that. Following the activation of the green LED, voters are now able to cast their ballots by pressing the designated key, which in this instance is the RED bread board 9 key.

The message "Already Voted" will now be displayed by the system for anyone who is attempting to cast a second ballot. Immediately following the ringing of the buzzer, the voter will no longer be able to cast their ballot after five seconds have passed. "No Fingerprint Found" will be displayed on the LCD display in the event that an unregistered user attempts to cast a ballot. This is because the fingerprint module is unable to recognize the user's identification within the system.

4. Results and Discussions

4.1. Designed Model

Electronic voting machines, which register votes electronically and eliminate the need for ballot paper, are a sight most people are familiar with.

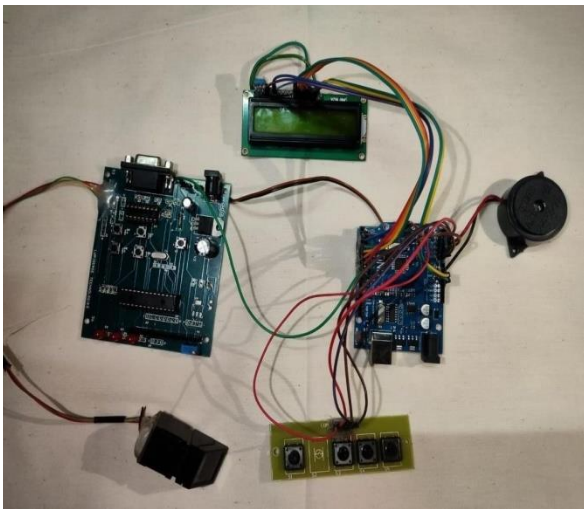

Figure 3. Designed Model

Fingerprint-based voting, in which a voter is granted authorization based only on his fingerprint, is a solution to the problem of double voting, which is a major security concern these days. Also, it will put an end to bogus votes. Therefore, we are using Arduino to build a biometric voting machine based on fingerprints today.

Fingerprint Recognition Accuracy: Evaluate the accuracy of the finger print recognition system. Include statistics on successful and unsuccessful recognition attempts. Discuss any challenges faced during the testing phase.

Voting Process: Describe the functionality of the electronic voting machine during the voting process. Include details on how voters interact with the system, verify their identity using fingerprints, and cast their votes electronically.

Vote Counting: Present the efficiency of the vote counting mechanism. Discuss how the Arduino UNO processes and stores votes securely. Highlight any security measures implemented to prevent tampering or manipulation of the vote count.

User Interface: Evaluate the user interface of the electronic voting machine. Discuss the ease of use for both voters and election officials. Consider factors such as clarity of instructions, feedback provided during the voting process, and any user-friendly features.

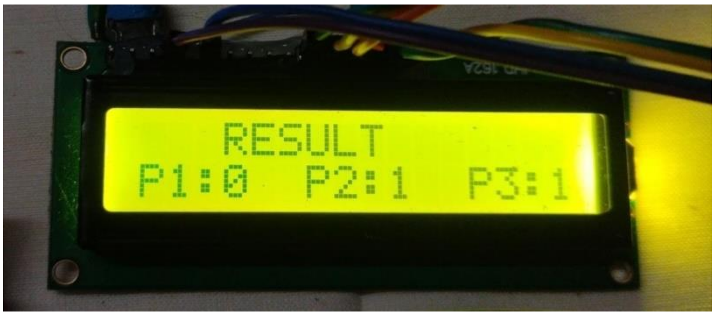

Figure 4. Final Vote Status

Arduino UNO Performance: Discuss the performance of Arduino UNO in handling the entire voting process. Comment on its processing speed, memory usage, and any limitations encountered. Explore whether it meets the demands of a real-world voting scenario.

Security Measures: Evaluate the security features implemented to prevent tampering or unauthorized access. This includes encryption of fingerprint data and secure storage of voting records.

4.2. Applications of Proposed System

Implementing expedited voting procedures could be advantageous for conducting elections on a smaller scale, such as those held by resident welfare associations, panchayats, and other societal organizations. This approach would enable immediate determination of election outcomes. Additionally, it could be utilized to carry out opinion surveys during the yearly shareholders' meeting. In the present circumstances, this technology could be employed for organizing local elections with a maximum of eight candidates.

4.3. Advantages

Cost-Effective: Arduino UNO is relatively inexpensive compared to dedicated hardware for EVMs, making it a cost-effective choice for developing voting systems.

Open Source: Arduino is an open-source platform, allowing developers to access and modify the source code. This transparency can enhance trust in the voting system, as the code can be scrutinized for security and fairness.

Customizability: Arduino UNO provides flexibility in designing custom features tailored to specific voting requirements. This adaptability ensures that the EVM can meet diverse electoral needs.

Portability: The compact size of Arduino UNO allows for the development of portable and lightweight EVMs. This is advantageous for deploying voting systems in diverse locations and settings.

Scalability: Arduino UNO can be scaled for larger voting systems by integrating it with other Arduino boards or microcontrollers. This scalability is crucial for accommodating elections of varying scales.

Ease of Programming: Arduino programming is user-friendly and supported by a large community. This makes it easier for developers to program and troubleshoot the EVM software, ensuring a reliable and efficient voting process.

User Interface: Arduino UNO can be paired with user-friendly interfaces, such as LCD displays and keypads, to provide a simple and intuitive experience for voters. This can reduce the likelihood of errors during the voting process.

Power Efficiency: Arduino UNO is designed to be power-efficient, which is crucial for EVMs, especially in areas with unreliable power sources. Low power consumption ensures that the EVMs can operate for extended periods.

Reliability: Arduino UNO is known for its reliability and durability. When used in EVMs, this reliability contributes to the overall stability of the voting system, minimizing the risk of technical failures during elections.

It’s important to note that while Arduino UNO offers these advantages, the development of an electronic voting system requires careful consideration of security measures to prevent tampering and ensure the integrity of the electoral process

5. Conclusion

Fingerprints have been one of the most popular ways to identify people for more than a century; automated biometric systems have only recently become accessible. The work was executed and assessed successfully. The ultimate results were more comparable and remarkable. This clearly illustrates that the process of enhancing the fingerprint image will unquestionably improve the verification performance of the fingerprint-based recognition system. Fingerprints will remain in use for both existing and new government systems, particularly in applications that demand a reliable biometric solution. This is due to the widespread acceptance of fingerprints among the general public, law enforcement agencies, and the forensic science community. This biometric voting system has the potential to facilitate fair elections in India. This measure will effectively prevent illicit activities, such as rigging. The citizens can be assured that they have exclusive authority to select their leaders, thereby exercising their democratic right.

Declarations

Source of Funding

The study has not received any funds from any organization.

Competing Interests Statement

The authors have declared no competing interests.

Consent for Publication

The authors declare that they consented to the publication of this study.

Authors' Contributions

All the authors took part in literature review, research, and manuscript writing equally.

References

[1] Vishal Vilas, N. (2014). Smart-Voting using Biometric. International Journal of Emerging Technology and Advanced Engineering, 4(6).

[2] Khasawneh, M., Malkawi M., & AlJarrah, O. (2008). A Biometric-Secure e-Voting System for Election Process. Proceeding of the 5th International Symposium on Mechatronics and its Applications (ISMA08), Amman, Jordan.

[3] Pajany, M., Kumar, K.S., Kumar, T.A., Rajmohan, R., & Ram, K.G. (2023). Enhancing Irrigation Efficiency with AI-Based Instinctive Irrigation System (IIS) in Wireless Sensor Networks. In 2023 International Conference on System, Computation, Automation and Networking, Pages 1–7, IEEE.

[4] Virendra Kumar Yadav, Saumya Batham, Mradul Jain & Shivani Sharma (2014). An Approach to Electronic Voting System using UIDAI. International Conference on Electronics and Communication Systems.

[5] Chaum, D.L. (1981). Untraceable Electronic Mail, Return Addresses and Digit Pseudonyms. Communications of the ACM, 24(2): 84–88.

[6] Janarthanan, M., Reddy, M.V.T., Reddy, C.R.S., Reddy, N.V., & Nikhil, K. (2019). Aadhar Based Electronic Voting Machine. In Journal of Physics: Conference Series, Volume 1362, Issue 1, Page 012050, IOP Publishing.

[7] Suresh Kumar, K., Gayathri, G., Arthi, A., & Sathishkumar, V. (2023). Artificial Intelligence Supported Instinctive Irrigation System (IIS) Using Arduino and ZigBee in Wireless sensor Network. International Journal of Advanced Research Trends in Engineering and Technology, 10(6): 1–11.

[8] Ashok, Kumar, D., & Ummal Begum, T. (2011). A novel design of electronic voting system using fingerprint.

[9] Jefferson, D., Rubin, A., Simons, B., & Wagner, D. (2009). A Security Analysis of the Secure Electronic Registration and Voting Experiment (SERVE). Technical Report Available at: http://www.servesecurityreport.org.

[10] Qijun Zhao, Lei Zhang, David Zhang & Nan Luo (2008). Adaptive pore model for fingerprint pore extraction. Proc. IEEE, 978-1-4244- 2175-6/08.

[11] Moheb R. Girgis, Tarek M. Mahmoud & Tarek Abd-El-Hafeez (2007). An Approach to Image Extraction and Accurate Skin Detection from Web Pages. World academy of Science, Engineering and Technology, Page 27.

[12] Kabilan, M., Manikandan, V., & Suresh Kumar, K. (2023). Synergizing IoT, IoE, GSM Technology, and Deep Learning Models for Advanced Security Applications: A Comprehensive Overview. Irish Interdisciplinary Journal of Science & Research, 7(4): 38–46.

[13] Manvjeet Kaur, Mukhwinder Singh, Akshay Girdhar & Parvinder S. Sandhu (2008). Fingerprint Verification System using Minutiae Extraction Technique. World academy of Science, Engineering and Technology, Page 46.

[14] Hoi Le & The Duy Bui (2009). Online fingerprint identification with a fast and distortion tolerant hashing. Journal of Information Assurance and Security, 4: 117–123.

[15] Mayank Vatsa, Richa Singh, Afzel Noore & Sanjay K. Singh (2009). Combining pores and ridges with minutiae for improved fingerprint verification. Signal Processing, 89: 2676–2685.

[16] Singh, B., Ranjan, K.S., & Aggarwal, D. (2020). Smart voting web based application using face recognition, Aadhar and OTP verification. International Journal of Research in Industrial Engineering, 9(3): 260–270.

[17] Kumar, S.A., Marzooq, A.M., Ranjithkumar, U., Romario, S., & Surya, P. (2023). Online Smart Voting System using Face Recognition. International Journal of Innovative Science and Research Technology, 8(3).

[18] Bhuvaneswary, N., Reddy, C.V., Aravind, C., & Prasad, K.H. (2022). Smart Voting Machine using Fingerprint Sensor and Face Recognition. In 2022 International Conference on Applied Artificial Intelligence and Computing (ICAAIC), Pages 1159–1166, IEEE.

[19] Kandan, M., Devi, K.D., Sri, K.D.N., Ramya, N., & Vamsi, N.K. (2021). Smart Voting System using Face Detection and Recognition Algorithms. In 2021 IEEE International Conference on Intelligent Systems, Smart and Green Technologies (ICISSGT), Pages 202–206, IEEE.

[20] Kumar, Akshay, Pooja Joshi, Jyotshana Kanti & Ahmed Alkhayyat (2023). Smart voting through face recognition. In AIP Conference Proceedings, Volume 2930, Number 1, AIP Publishing.

[21] Manju Payal, Ananth Kumar, T., & Suresh Kumar, K. (2022). Machine Learning in Industry 4.0. International Journal of Innovative Research in Science, Engineering and Technology, 11(5): 5831–5840.

[22] Thamaraimanalan, T., Jayaprada, D., Dhavasree, S., Kasthuri, K., & Deenathayalini, M. (2017). Aadhar Based Electronic Voting Machine. Asian Journal of Applied Science and Technology, 1(2).

[23] Gupta, S., Jain, D., & Themalil, M.T. (2021). Electronic Voting Mechanism using Microcontroller ATmega32 8P with Face Recognition. In 2021 5th International Conference on Computing Methodologies and Communication (ICCMC), Pages 1471–1476, IEEE.

[24] Khan, S. (2020). Smart Voting System Support through Face Recognition.